REPRÉSENTATION DE – 1 COMME SOMME DE CARRÉS D'ENTIERS DANS UN CORPS QUADRATIQUE IMAGINAIRE

Autor(en): **Moser, C.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **17 (1971)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-44582

REPRÉSENTATION DE -1 COMME SOMME DE CARRÉS D'ENTIERS DANS UN CORPS QUADRATIQUE IMAGINAIRE

par C. MOSER

INTRODUCTION

On se propose dans cet article de déterminer le plus petit nombre de carrés nécessaires pour représenter -1 dans l'anneau A_m des entiers d'un corps quadratique imaginaire $\mathbf{Q}(\sqrt{-m})$. De façon précise, on montre que ce nombre de carrés (« Stufe » de A_m dans la terminologie traditionnelle; notation $s(A_m)$) vaut 1 si $m = 1$, 4 si $m \equiv 7 \pmod 8$, 2 ou 3 lorsque $m \not\equiv 3 \pmod 4$, selon que la norme de l'unité fondamentale ε_m du corps quadratique réel $\mathbf{Q}(\sqrt{m})$ est -1 ou $+1$; enfin, dans le cas $m \equiv 3 \pmod 8$, $s(A_m)$ vaut 2 ou 3 selon que $u_m - 1$ est un carré ou non, u_m désignant la partie rationnelle de l'unité ε_m. Ainsi il est possible, à l'aide d'une table des unités des corps quadratiques réels, de déterminer explicitement $s(A_m)$ pour tout corps quadratique imaginaire $\mathbf{Q}(\sqrt{-m})$.

En fait, les démonstrations que nous donnons, et qui sont entièrement élémentaires, permettraient, pour m donné, et connaissant la valeur numérique de ε_m, de déterminer une représentation effective de -1 comme somme de $s(A_m)$ carrés dans l'anneau A_m.

Les résultats présentés ici ont été annoncés dans [1]. Signalons d'autre part que M. Kneser, P. Draxl et M. Peters (voir [2], [3]) viennent d'obtenir une méthode générale permettant d'évaluer la « Stufe » $s(A)$ d'un ordre d'entiers algébriques (totalement imaginaire) quelconque: cette méthode utilise certains résultats de M. Eichler [5] et le théorème d'Approximation de M. Kneser [6], et fait donc intervenir des considérations locales.

NOTATIONS

Dans tout ce qui suit nous désignons par

m	un entier rationnel ≥ 1 et sans facteur carré;
K_m	le corps quadratique *imaginaire* $\mathbf{Q}(\sqrt{-m})$;
L_m	le corps quadratique *réel* $\mathbf{Q}(\sqrt{m})$;

N	l'application norme dans l'extension $L_m/\mathbf{Q}$;
E_m	le corps biquadratique composé de L_m et K_m;
ε_m	l'unité fondamentale de L_m, $\varepsilon_m = u_m + v_m\sqrt{m}$;
A_m	l'anneau des entiers de K_m;
$s(A_m)$	la « Stufe » de A_m, c'est-à-dire le plus petit entier s tel que -1 soit somme de s carrés dans A_m;
$s(\mathbf{Z}[\sqrt{-m}])$	la « Stufe » de l'ordre $\mathbf{Z}[\sqrt{-m}]$.

1. *Détermination de $s(A_m)$ lorsque $m \equiv 7 \pmod 8$.*

THÉORÈME 1.

Si m est congru à 7 modulo 8, alors $s(A_m) = 4$.

Démonstration :

En effet, $m - 1 \equiv 6 \pmod 8$ est alors somme de trois carrés dans $\mathbf{Z}$: $m - 1 = a^2 + b^2 + c^2$, et par suite $-1 = a^2 + b^2 + c^2 + (\sqrt{-m})^2$ est somme de quatre carrés dans $\mathbf{Z}[\sqrt{-m}] = A_m$. Si on avait $s(A_m) \leq 3$, il existerait six nombres entiers $x_1, x_2, x_3, y_1, y_2, y_3$ tels que

$$-1 = \sum_1^3 (x_i + y_i\sqrt{-m})^2 ,$$

c'est-à-dire $-1 = \sum_1^3 x_i^2 - my_i^2$ et $0 = \sum_1^3 x_i y_i$. Du fait que $m \equiv -1 \pmod 8$, il résulterait de ces deux égalités (en multipliant la seconde par 2 et en l'ajoutant à la première):

$$-1 \equiv \sum_1^3 (x_i + y_i)^2 \pmod 8 .$$

Or il est bien connu que -1 n'est pas somme de trois carrés dans $\mathbf{Z}/8\mathbf{Z}$. Par conséquent, $s(A_m) = 4$.

2. *Détermination de $s(A_m)$ lorsque $m \not\equiv 3 \pmod 4$.*

LEMME 1.

Soit γ_m l'unité fondamentale de $\mathbf{Z}[\sqrt{m}]$, $(m > 1)$. Alors $\gamma_m = \varepsilon_m$, sauf si m est congru à 1 modulo 4, auquel cas $\gamma_m = \varepsilon_m$ ou $\gamma_m = \varepsilon_m^3$.

Démonstration:

Si $m \not\equiv 1 \pmod 4$, l'anneau des entiers de $L_m = \mathbf{Q}(\sqrt{m})$ est $\mathbf{Z}[\sqrt{m}]$. Si $m \equiv 1 \pmod 4$, on sait que $2\varepsilon_m = a + b\sqrt{m}$ avec $a \equiv b \pmod 2$ et $a^2 - mb^2 = \pm 4$. On a alors si $a \equiv b \equiv 1 \pmod 2$

$$\varepsilon_m^2 = \pm 1 - \frac{mb^2}{2} + \frac{ab\sqrt{m}}{2} \notin \mathbf{Z}[\sqrt{m}] .$$

et

$$\varepsilon_m^3 = a\left(\frac{mb^2 \pm 1}{2}\right) + \left(\frac{a^2 \pm 1}{2}\right) b\sqrt{m} \in \mathbf{Z}[\sqrt{m}] .$$

ce qui démontre le lemme.

Proposition 1.

Soit $m \geq 1$ un entier sans facteur carré et non congru à 7 modulo 8. Alors

i) *si* $m = 1$, $s(\mathbf{Z}[\sqrt{-m}]) = 1$

ii) *si* $m > 1$ *et* $N(\varepsilon_m) = -1$, $s(\mathbf{Z}[\sqrt{-m}]) = 2$

iii) *si* $m > 1$ *et* $N(\varepsilon_m) = +1$, $s(\mathbf{Z}[\sqrt{-m}]) = 3$

Démonstration:

Pour i), il n'y a rien à démontrer. ii) est une conséquence du lemme 1, car si $\gamma_m = a_m + b_m\sqrt{m}$ avec $a_m, b_m \in \mathbf{Z}$, on a

$$N\gamma_m = N\varepsilon_m^3 = N\varepsilon_m = -1$$

et

$$-1 = a_m^2 + (b_m\sqrt{-m})^2 .$$

Démontrons iii) en deux étapes:

1) $s(\mathbf{Z}[\sqrt{-m}]) \geq 3$. Il suffit de montrer que l'équation

$$(E) \qquad -1 = (x_1 + y_1\sqrt{-m})^2 + (x_2 + y_2\sqrt{-m})^2$$

n'a pas de solutions en nombres entiers x_1, x_2, y_1, y_2. Or cette équation est équivalente au système d'équations:

$$(S_1) \qquad \begin{cases} -1 = x_1^2 + x_2^2 - m(y_1^2 + y_2^2) \\ 0 = x_1y_1 + x_2y_2 . \end{cases}$$

Du fait que $N\varepsilon_m = +1$, le système (S_1) n'admet pas de solution entière telle que $x_1 x_2 = 0$. Ce système est donc équivalent au suivant

$$(S_2) \qquad \begin{cases} x_2^2 = (x_1^2 + x_2^2)(my_1^2 - x_2^2) \\ 0 = x_1 y_1 + x_2 y_2 \\ x_1 x_2 \neq 0 \end{cases}$$

dont la première équation n'admet évidemment pas de solution entière non triviale. Par conséquent $s(\mathbf{Z}[\sqrt{-m}]) \geq 3$.

2) $s(\mathbf{Z}[\sqrt{-m}]) \leq 3$. Remarquons que $m \not\equiv 7 \pmod 8$ est somme de deux ou de trois carrés dans $\mathbf{Z}$ et distinguons ces deux cas (encore que le premier soit évidemment contenu dans le second):

— si $m = a^2 + b^2$, on a évidemment $(a, b) = 1$. D'après l'identité de Bezout, il existe deux entiers y_1 et y_2 tels que $ay_1 + by_2 = 1$;
on peut alors écrire

$$m(y_1^2 + y_2^2) = 1 + (ay_2 - by_1)^2 ,$$

d'où la représentation

$$-1 = (ay_2 - by_1)^2 + (y_1\sqrt{-m})^2 + (y_2\sqrt{-m})^2 .$$

— si $m = a^2 + b^2 + c^2$, on a $(a, b, c) = 1$; toujours d'après l'identité de Bezout, il existe trois entiers y_1, y_2, y_2 tels que $ay_1 + by_2 + cy_2 = 1$. Utilisons ici la multiplicativité de la norme des quaternions. Nous obtenons

$$\begin{aligned} m(y_1^2 + y_2^2 + y_3^2) = {} & (ay_1 + by_2 + cy_3)^2 + (by_1 - ay_2)^2 \\ & + (cy_1 - ay_3)^2 + (cy_2 - by_3)^2 ; \end{aligned}$$

il en résulte

$$\begin{aligned} -1 = {} & (by_3 - cy_2 + y_1\sqrt{-m})^2 + (cy_1 - ay_3 + y_2\sqrt{-m})^2 \\ & + (ay_2 - by_1 + y_3\sqrt{-m})^2 . \end{aligned}$$

Ces deux calculs montrent de façon explicite que $s(\mathbf{Z}[\sqrt{-m}]) = 3$.

THÉORÈME 2.

Si $m > 1$ est non congru à 3 modulo 4, *alors $s(A_m) = 2$ ou 3 selon que $N\varepsilon_m = -1$ ou $+1$.*

Démonstration :

Il suffit de remarquer que, comme $-m \not\equiv 1 \pmod 4$, on a $A_m = \mathbf{Z}[\sqrt{-m}]$, et d'appliquer la proposition 1.

3. *Détermination de $s(A_m)$ lorsque $m \equiv 3 \pmod 8$.*

Dans le dernier cas qui nous reste à étudier nous aurons besoin de quelques résultats supplémentaires sur les unités de L_m.

LEMME 2.

Soit $m > 1$ un entier sans facteur carré tel que $N\varepsilon_m = 1$. Les trois assertions suivantes sont équivalentes :

i) *$i\gamma_m$ est un carré dans $E_m = \mathbf{Q}(\sqrt{m}, \sqrt{-m})$, $i = \sqrt{-1}$;*

ii) *$2\gamma_m$ est un carré dans $\mathbf{Z}[\sqrt{m}]$;*

iii) *Si on pose $\gamma_m = a_m + b_m\sqrt{m}$, $(a_m, b_m \in \mathbf{Z})$, alors l'un des nombres $a_m + 1$, $a_m - 1$ est un carré dans $\mathbf{Z}$.*

Démonstration :

Il suffit pour le voir de décomposer $i\gamma_m$ sur la $\mathbf{Q}$-base de E_m formée par $1, i, \sqrt{m}, \sqrt{-m}$.

Proposition 2.

Soit $m > 1$ un entier sans facteur carré tel que $N\varepsilon_m = +1$. Alors, si $s(A_m) = 2$, l'un des nombres $a_m + 1$, $a_m - 1$ est un carré dans $\mathbf{Z}$.

Démonstration :

D'après le lemme 2, il suffit de montrer que $i\gamma_m$ (ou a fortiori $i\varepsilon_m$) est un carré dans E_m. Le corps E_m est une extension biquadratique non réelle du corps $\mathbf{Q}$ dont les sous-corps quadratiques sont K_m, L_m et $\mathbf{Q}(i)$.

Il résulte du théorème de Dirichlet que le groupe des unités de E_m est de rang 1, donc isomorphe au groupe $W_m \times \mathbf{Z}$, où W_m est le groupe des racines de l'unité du corps E_m. Un calcul de degrés montre que $W_m = \{\pm 1, \pm i\}$ dès que $m > 6$. Par ailleurs, il est bien connu (voir les tables) que $N\varepsilon_2 = N\varepsilon_5 = -1$ et que $N\varepsilon_3 = N\varepsilon_6 = 1$ et le théorème 2 nous montre que $s(A_6) = 3$. Dans le cas $m = 3$, on a $\varepsilon_3 = 2 + \sqrt{3}$, $a_3 = 2$ et $a_3 - 1 = 1$ est un carré. La proposition est donc vraie pour

$m \leq 6$ et on peut supposer dans la suite de cette démonstration que $m > 6$ et $W_m = \{ \pm 1, \pm i \}$. Soit alors η_m l'unité fondamentale de E_m. Il existe a et $b \in \mathbf{Z}$ tels que $\varepsilon_m = i^a \eta_m^b$. Soit N^* l'application norme dans l'extension E_m/K_m. Il résulte de la théorie de Galois que pour tout $x \in L_m$ on a $Nx = N^*x$. En particulier:

$$1 = N\varepsilon_m = (N^*\eta_m)^b .$$

Dans ces conditions, si $s(A_m) = 2$, -1 est la norme d'une unité de E_m dans l'extension E_m/K_m et le nombre b est pair. Il en résulte que ε_m est de l'une des quatre formes $\pm \eta_m^{2p}$, $\pm i \eta_m^{2p}$ ($p \in \mathbf{Z}$). Raisonnons par l'absurde et supposons que $\varepsilon_m = \pm \eta_m^{2p}$. Cette hypothèse implique que ε_m est un carré dans E_m, donc que $\mathbf{Q}(\sqrt{\varepsilon_m})$ est un sous-corps de E_m. Le corps $\mathbf{Q}(\sqrt{\varepsilon_m})$ est réel. C'est donc un sous-corps de L_m qui est le sous-corps réel maximal de E_m. Ce résultat contredit le fait que ε_m est l'unité fondamentale de L_m. Par conséquent ε_m est de la forme $\pm i\eta_m^{2p}$, $i\varepsilon_m = \pm \eta_m^{2p}$ est bien un carré dans E_m, et la proposition est démontrée.

THÉORÈME 3.

Soit $m > 1$ un entier sans facteur carré et congru à 3 modulo 8. Les trois assertions suivantes sont équivalentes :

i) $s(A_m) = 2$;

ii) *l'équation $x^2 - my^2 = -2$ admet une solution en nombres entiers x, y;*

iii) *si on pose $\varepsilon_m = u_m + v_m\sqrt{m}$, alors $u_m - 1$ est un carré dans $\mathbf{Z}$.*

Si ces conditions ne sont pas réalisées, alors $s(A_m) = 3$.

Démonstration:

Puisque $m \equiv 3 \pmod 8$, il existe un diviseur premier $p \equiv 3 \pmod 4$ de m. De ce fait on a $N\varepsilon_m = +1$, car -1 n'est pas reste quadratique modulo p. En particulier $s(\mathbf{Z}[\sqrt{-m}]) = 3$ d'après la proposition 1. A fortiori, $s(A_m) \leq 3$, et il reste à prouver l'équivalence de i), ii) et iii).

i) *implique* ii). Si $s(A_m) = 2$, il existe quatre entiers rationnels x_1, x_2, y_1, y_2 tels que $x_1 \equiv x_2 \equiv y_1 \equiv y_2 \equiv 1 \pmod 2$ avec $-4 = (x_1 + y_1\sqrt{-m})^2 + (x_2 + y_2\sqrt{-m})^2$. Il en résulte l'égalité

$$-4x_2^2 = (x_1^2 + x_2^2)(x_2^2 - my_1^2) .$$

Ceci n'est évidemment possible que si $x_1^2 + x_2^2 = 2x_2^2$ et $x_2^2 - my_1^2 = -2$, d'où ii).

ii) *implique* i). Soient x, $y \in \mathbf{Z}$ tels que $x^2 - my^2 = -2$. Les entiers x et y sont nécessairement impairs et on a

$$-1 = \left(\frac{x+y\sqrt{-m}}{2}\right)^2 + \left(\frac{x-y\sqrt{-m}}{2}\right)^2,$$

d'où i).

i) *implique* iii). D'après la proposition 2, il suffit de montrer que $u_m + 1$ ne peut pas être un carré dans $\mathbf{Z}$. S'il en était ainsi, l'égalité $u_m^2 - 1 = mv_m^2$ impliquerait l'existence de deux entiers a et b tels que $u_m - 1 = ma^2$ et $u_m + 1 = b^2$, c'est-à-dire $b^2 - ma^2 = 2$. Puisque i) et ii) sont équivalents, il existe par ailleurs deux entiers c et d tels que $c^2 - md^2 = -2$. On vérifierait alors que $(c+d\sqrt{m})\,(a+b\sqrt{m})^{-1}$ est une unité de norme -1 dans L_m. Mais ceci est impossible (voir le début de la démonstration).

iii) *implique* ii). On a $(u_m+1)\,(u_m-1) = mv_m^2$. Si $u_m - 1$ est un carré d'entier, soit $u_m - 1 = b^2$, alors $u_m + 1 = ma^2$, $a \in \mathbf{Z}$, et on a bien

$$-2 = (u_m-1) - (u_m+1) = a^2 - mb^2 .$$

Le théorème est ainsi démontré.

4. *Quelques applications.*

Proposition 3.

Si m est un nombre premier, on a $s(A_m) = 2$, sauf si $m \equiv 7 \pmod 8$, auquel cas $s(A_m) = 4$.

Démonstration :

Le cas $m = 2$ ayant déjà été examiné, on peut supposer m premier *impair*.

Si $m \equiv 1 \pmod 4$, la théorie des genres (voir par exemple [6]) montre que $N\varepsilon_m = -1$. On applique alors le théorème 2.

Si $m \equiv 3 \pmod 8$, il suffit de montrer que $u_m - 1$ est un carré dans $\mathbf{Z}$. A priori, quatre cas peuvent se présenter:

a) $u_m + 1$ est un carré;

b) $u_m + 1$ est le double d'un carré;

c) $u_m - 1$ est le double d'un carré;

d) $u_m - 1$ est un carré.

Eliminons les trois premiers. L'hypothèse a) impliquerait que $\frac{1}{m}(u_m - 1)$ est un carré et que 2 est reste quadratique modulo m, ce qui est faux. L'hypothèse b) impliquerait que $\frac{1}{2m}(u_m - 1)$ est un carré; il existerait deux entiers x et y tels que $0 < x < u_m$ et $x^2 - my^2 = 1$; mais ceci contredirait le fait que $\varepsilon_m = u_m + v_m\sqrt{m}$ est l'unité fondamentale de L_m. L'hypothèse c) impliquerait que $\frac{1}{2m}(u_m + 1)$ est un carré dans $\mathbf{Z}$; -1 serait donc norme d'un entier de L_m, ce qui est absurde. Seul le cas d) est possible et donc, d'après le théorème 3, $s(A_m) = 2$.

Enfin, si $m \equiv 7 \pmod 8$, on applique le théorème 1.

Proposition 4.

Il existe une infinité d'entiers m tels que $s(A_m) = 3$.

Démonstration :

Il suffit de considérer les entiers m qui sont produit en nombre pair de nombres premiers congrus à 3 (mod 4), ou les entiers m qui sont produit d'un nombre premier congru à 5 (mod 8) par un nombre premier congru à 7 modulo 8 (un tel entier m n'est pas représentable rationnellement par la forme quadratique $X^2 + 2Y^2$, et l'équation $-2 = x^2 - my^2$ n'a donc pas de solution en nombres entiers x, y).

BIBLIOGRAPHIE

[1] Moser, C., « Représentation de -1 par une somme de carrés dans certains corps locaux et globaux, et dans certains anneaux d'entiers algébriques », *C. R. Acad. Sci.*, Paris, *271* (1970), pp. 1200-1203.

[2] Draxl, P., « Représentation de -1 comme somme de carrés dans les ordres d'un corps de nombres algébriques », *Journées Arithmétiques de Marseille*, mai 1971.

[3] Peters, M., « Die Stufe von Ordnungen ganzer Zahlen in algebraischen Zahlkörpern », à paraître dans *Math. Annalen.*

[4] Eichler, M., « Die Ähnlichkeitsklassen indefiniter Gitter », *Math. Z.*, *55* (1952), pp. 216-252.

[5] KNESER, M., « Klassenzahlen indefiniter quadratischen Formen in drei order mehr Veränderlichen », *Arch. Math.*, *7* (1956), pp. 323-332.

[6] BOREVITCH, Z. I. et I. R. SHAFAREVICH, « Number Theory », *Academic Press* (notamment p. 248).

(Reçu le 26 août 1971)

C. Moser
Institut de Mathématiques Pures
Boîte postale 116
38 — Saint-Martin d'Hères